UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,659	02/18/2004	Tatsunori Kanai	04284.0880	8931

22852 7590 11/26/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SHAIFER HARRIMAN, DANT B	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
11/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,659	KANAI ET AL.	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/18/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/14/2005, 02/14/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 11 – 18 & 23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*. Furthermore, the claim limitations "program" and "code" suggest

software to the examiner, thus as explained above, software is clearly not a statutory subject matter.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claim(s) 1 - 25 are rejected under 35 U.S.C. 102(b) as being taught by Downs et al. (US Patent NO. 6226618 B1).

Downs teaches:

Claim # 1. A server apparatus comprising:

- a key sharing processing unit configured to perform a first protocol to share a first key with a client apparatus (please see the abstract of reference & Col. 42, lines 37 - 47, the examiner notes that the clearing house is the "key sharing processing unit," that sends an encrypted data decrypting key along with the encrypted data to the user's system, furthermore the examiner notes that the secure content digital electronic distribution system is implemented through a website or sites, that reside on a server, the server on which the secure content digital electronic distribution system is what the examiner considers a "server apparatus.");

- an encryption/decryption unit configured to encrypt data or decrypt encrypted data by use of the first key obtained from said key sharing processing unit (please see the abstract of

the reference, the examiner notes that the clearing house "re-encrypts" the decrypted encrypted information and corresponding key, and then it is sent to the user's system.);

- a communication unit configured to transmit to said client apparatus, data which was encrypted by said encryption/decryption unit or receive from said client apparatus, data which was encrypted by using the first key (please see the abstract of reference, the examiner notes that the clearing house is the "key sharing processing unit," that sends an encrypted data decrypting key along with the encrypted data to the user's system); and

said key sharing processing unit having:

- a first reception unit configured to receive key information from said client apparatus, said key information including the first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (please see the references abstract, the examiner notes that the client apparatus or user's system has public/private key pair (Col. 82, lines 40 – 52) that allows the user to encrypt the communications with the clearinghouse which also has private/public key pair, furthermore, clearing house "re-encrypts" the decrypted encrypted information and corresponding decryption key with a second public key, and then it is sent to the user's system, the "second public key" is the actual "second key"),

- a transmission unit configured to transmit a request to decrypt the key information to a key management apparatus

which maintains a third key necessary for decrypting the key information (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content); and

- a second reception unit configured to receive the first key or the data which becomes a basis for generating the first key from said key management apparatus (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content after it has been authorized).

Claim #2. The server apparatus according to claim 1, further comprising

- a key generation unit configured to generate the first key, from the data which becomes a basis for generating the first key (please see the abstract of reference, the examiner notes that the clearing house is the "key generation unit," that sends an encrypted data decrypting key along with the encrypted data to the user's system).

Claim #3. The server apparatus according to claim 1, wherein

- a connection between said server apparatus and said key management apparatus is through a dedicated network isolated from said client apparatus (Col. 8, lines 42 – 45 & Col. 23, lines 1 - 20).

Claim #4. The server apparatus according to claim 1, wherein

- data transferred to said key management apparatus is encrypted before transfer (please see the reference abstract, the examiner notes that the Electronic Digital Content Store sends the requested content to the clearinghouse with a first public key, then the clearing house decrypts the content and the decrypting encrypted data key with a first private key, then the clearinghouse re-encrypts the data and decrypting key with a second public key.

Claim #5. The server apparatus according to claim 4, wherein

- a second protocol for sharing a fourth key which is used for encrypting data transferred to said key management apparatus is as same as the first protocol (Col. 82, lines 40 52, the examiner notes that when the "player application" is installed on the user's system or device, a public/private key pair is also installed on the user's device. This will allow the

user to send a encrypted message or content to the clearing house to report technical player application errors, without the player or requested content from being compromised).

Claim #6. The server apparatus according to claim 1, wherein

- said transmission unit transmits all requests to one predetermined key management apparatus (Col. 8, lines 7 – 11 & Col. 10, lines 50 - 65).

Claim #7. The server apparatus according to claim 1, wherein

- said transmission unit transmits the request to one predetermined key management apparatus selected from a plurality of key management apparatuses (Col. 11, lines 16 – 29, the examiner notes that if the user requests digital

content through a website then depending on where the particular requested content is stored, it could be available on several Electronic Content Stores or only on one electronic content store, furthermore attached to each electronic content store is a clearinghouse, the clearinghouse is what the examiner considers a "key management apparatus," thus their must be more than one clearinghouse).

Claim #8. The server apparatus according to claim 1, further comprising

- a storing unit configured to store authentication information used to authenticate said server apparatus with said client apparatus (Col. 7, lines 2 – 10, the secure digital content distribution system, specifically the clearinghouse authorizes the user's request to obtain rights to download and view the

requested digital content).

Claim #9. The server apparatus according to claim 1, further comprising

- an obtaining unit configured to obtain authentication information used for server authentication with said client apparatus from said key management apparatus (Col. 7, lines 2 – 10, the secure digital content distribution system, specifically the clearinghouse authorizes the user's request to obtain rights to download and view the requested digital content).

Claim #10. The server apparatus according to claim 1, wherein

- the server apparatus stores the second key temporarily, but does not stores the third key at anytime (please see the reference abstract, the examiner notes that Electronic

Content store, encrypts the data and decryption key with a first public key, to which their is a first private key (i.e. the second key), which is stored on the clearinghouse, the third key is the actual decryption key that is used to decrypt the encrypted data).

Claim #11. A key management apparatus comprising:

- a reception unit configured to receive a request for decrypting key information from a server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital

content after it has been authorized, furthermore clearing house "re-encrypts" the decrypted encrypted information and corresponding decryption key with a second public key, and then it is sent to the user's system, the "second key" is the actual decryption key of the encryption key);

- a storing unit configured to store a third key which is necessary for decrypting the key information (please see the abstract of reference, the examiner notes that the Electronic Content store, encrypts the data and decryption key with a first public key, to which their is a first private key (i.e. the second key), which is stored on the clearinghouse, the third key is the actual decryption key that is used to decrypt the encrypted data, the clearinghouse will "re-encrypt" the encryption decryption key and the data with a second public

key, and send it to the user's system);

- a decryption unit configured to decrypt the key information with the third key and obtain the first key or the data which becomes a basis for generating the first key, after receiving the request (please see the abstract of reference, the examiner notes that the user's system will have a second public key that can be used to allow the user's system to decrypt the digital content); and

- a transmission unit configured to transmit to said server apparatus the first key or the data which becomes a basis for generating the first key, wherein said server apparatus and a client apparatus are able to share the first key (Col. 12, lines 44 – 53 & Col. 15, lines 1 – 66 & Col. 16, lines 1 - 20).

Claim #12. The key management apparatus according to claim 11, wherein

- said key information is encrypted by said client apparatus (Col. 82, lines 40 - 52, the examiner notes that when the "player application" is installed on the user's system or device, a public/private key pair is also installed on the user's device. This will allow the user to send a encrypted message or content to the clearing house to report technical player application errors, without the player or requested content from being compromised).

Claim #13. The key management apparatus according to claim 11, wherein

- a connection between said key management apparatus and said server apparatus is through a dedicated network which is isolated from said client apparatus (Col. 8, lines 42 – 45 & Col. 23, lines 1 - 20).

Claim #14. The key management apparatus according to claim 11, wherein

- data to be transferred to said server apparatus is encrypted before transfer(please see the reference abstract, the examiner notes that the Electronic Digital Content Store sends the requested content to the clearinghouse with a first public key, then the clearing house decrypts the content and the decrypting encrypted data key with a first private key, then the clearinghouse re-encrypts the data and decrypting key with a second public key).

Claim #15. The key management apparatus according to claim 14, wherein

- a protocol for sharing a fourth key used to encrypt data transferred to said server apparatus is the same as a protocol for sharing said first key between said server apparatus and said client apparatus (Col. 82, lines 40 52, the examiner notes that when the "player application" is installed on the user's system or device, a public/private key pair is also installed on the user's device. This will allow the user to send a encrypted message or content to the clearing house to report technical player application errors, without the player or requested content from being compromised).

Claim #16. The key management apparatus according to claim 11, wherein

- the key management apparatus is connected to a plurality of server apparatuses, and the second key and the third key are commonly used for the plurality of server apparatuses (Col. 11, lines 16 – 28, the examiner notes that the "key management apparatus" is the clearinghouse, and the "server apparatus" is the Electronic Digital Content Store(s), the electronic digital content store is a website that is located on a content provider's server).

Claim #17. The key management apparatus according to claim 11, wherein

- the key management apparatus is connected to a plurality of server apparatuses, and the second key and the third key are unique to one server apparatus of the plurality of server

apparatus (Col. 10, lines 50 – 65, , the examiner notes that if the user requests digital content through a website then depending on where the particular requested content is stored, it could be available on several Electronic Content Stores or only on one electronic content store, furthermore attached to each electronic content store is a clearinghouse, the clearinghouse is what the examiner considers a "key management apparatus," thus their must be more than one clearinghouse, furthermore please see the reference abstract, the clearinghouse for every content provider will be different, thus the third and second keys will be different).

Claim #18. The key management apparatus according to claim 11, further comprising:

- a second storing unit configured to store authentication information which said server apparatus uses for server

authentication with said client apparatus (Col. 10, lines 50 – 65 & Col. 7, lines 1-10, the examiner notes that the clearing house will have a memory or storing unit to keep track of all transactions, and licensing authorization information in order to authorize a license to a end user, and also verify if the requested content and the information in the content request itself, as well as the verify the authorization of the content from the content providers);

- a second reception unit configured to receive, from said server apparatus, an authentication request for the authentication information (Col. 10, lines 50 – 65, the examiner notes that the clearing house will have a memory or storing unit to keep track of all transactions, and licensing authorization information in order to authorize a license to a end user, and also verify if the requested content and the

information in the content request itself, as well as the verify the authorization of the content from the content providers); and

- a second transmission unit configured to transmit the authentication information to said server apparatus, after receiving the authentication request (Col. 10, lines 50 – 65, the examiner notes that the clearing house will have a memory or storing unit to keep track of all transactions, and licensing authorization information in order to authorize a license to a end user, and also verify if the requested content and the information in the content request itself, as well as the verify the authorization of the content from the content providers).

Claim #19. An encrypted communication method comprising:

- receiving key information from a client apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (please see reference abstract);

- transmitting a request to decrypt the key information to a key management apparatus which stores a third key necessary for decrypting the key information (please see reference abstract);

- receiving the first key or the data which becomes a basis for generating the first key from said key management

apparatus(please see reference abstract);

- if the key information is a basis for generating the first key, generating the first key from the basis(please see reference abstract); and

- encrypting data using the first key and transmitting the data encrypted with the first key to said client apparatus, or receiving data encrypted with the first key from said client apparatus and decrypting the data encrypted with the first key(please see reference abstract).

Claim #20. The encrypted communication method according to claim 19, wherein

- encrypting said key information comprises using an asymmetric encryption process, and the second key is a

public key and the third key is a private key (please see the reference abstract).

Claim #21. An encrypted communication method comprising:

- receiving a request for decrypting key information from a server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (please see the reference abstract);

- storing a third key which is necessary for decrypting the key information(please see the reference abstract, the examiner notes that the clearinghouse has a first private key that is used to decrypt the encrypted data and the decrypting encryption data key);

- decrypting said key information with the third key and obtaining the first key or the data which becomes a basis for generating the first key, after receiving the request (please see the reference abstract); and

- transmitting to said server apparatus the first key or the data which becomes a basis for generating the first key, wherein the server apparatus and a client apparatus are able to share the first key (Col. 12, lines 44 – 53 & Col. 15, lines 1 – 66 & Col. 16, lines 1 - 20).

Claim #22. The encrypted communication method according to claim 21, wherein

- decrypting said key information comprises using an asymmetric decryption process, and the second key is a public key and the third key is a private key (please see the reference abstract).

Claim #23. A communication program for communicating to a client computer, comprising:

- a key sharing processing program code configured to perform a protocol for sharing a first key with a client computer (please see the abstract of reference & Col. 42, lines 37 - 47, the examiner notes that clearinghouse is a database server or PC that executes programs or code or instructions that implement the clearinghouse functions(Col. 43, lines 18 - 25) furthermore the clearing house is the "key sharing processing unit," that sends an encrypted data

decrypting key along with the encrypted data to the user's system, furthermore the examiner notes that the secure content digital electronic distribution system is implemented through a website or sites, that reside on a server, the server on which the secure content digital electronic distribution system is what the examiner considers a "server apparatus.");

- an encryption/decryption program code configured to encrypt data or decrypt encrypted data using of first key obtained from said key sharing processing program code (please see the abstract of the reference, the examiner notes that the clearing house “re-encrypts” the decrypted encrypted information and corresponding key, and then it is sent to the user's system.);

- a communication program code configured to transmit to Said client apparatus, data encrypted by said encryption/decryption program code or configured to receive, from said client apparatus, data which was encrypted using the first key (please see the abstract of reference, the examiner notes that the clearing house is the "key sharing processing unit," that sends an encrypted data decrypting key along with the encrypted data to the user's system); and

said key sharing processing program code having:

- a first reception program code configured to receive key information from said client apparatus, said key information including the first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (Col. 82, lines 40 – 52) that allows the user to encrypt the communications with the

clearinghouse which also has private/public key pair, furthermore, clearing house "re-encrypts" the decrypted encrypted information and corresponding decryption key with a second public key, and then it is sent to the user's system, the "second key" is the second public key);

- a transmission program code configured to transmit a request to decrypt the key information to a key management apparatus which stores a third key necessary for decrypting the key information (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content); and

- a second reception program code configured to receive the first key or the data which becomes a basis for generating

the first key from said key management apparatus (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content after it has been authorized).

Claim #24. A communication program for managing key information, comprising:

- a first reception program code configured to receive a request for decrypting key information from a server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with a second key (Col. 82, lines 40 – 52) that allows the user to encrypt the communications with the clearinghouse which also has private/public key pair, furthermore, clearing house "re-encrypts" the decrypted encrypted information and

corresponding decryption key with a second public key, and then it is sent to the user's system, the "second key" is the second public key;

- a first storing program code configured to store a third key necessary for decrypting the key information (please see the abstract of reference, the examiner notes that the Electronic Content store, encrypts the data and decryption key with a first public key, to which their is a first private key (i.e. the second key), which is stored on the clearinghouse, the third key is the actual decryption key that is used to decrypt the encrypted data, the clearinghouse will "re-encrypt" the encryption decryption key and the data with a second public key, and send it to the user's system);

- a decryption program code configured to decrypt said key information with the third key and obtain the first key or the data which becomes a basis for generating the first key, after receiving the request (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content); and

- a first transmission program code configured to transmit the first key or the data which becomes a basis for generating the first key to said server apparatus, wherein said server apparatus and a client apparatus are capable of sharing the first key (please see the abstract of reference & Col. 82, lines 40 – 52, the examiner notes that the user's system will want to decrypt the requested digital content).

Claim #25. A secure communication system, comprising:

- a network (Col. 8, lines 42 – 45 & Col. 23, lines 1 - 20);

- a server apparatus connected to said network and capable of exchanging data with a client apparatus, said server apparatus having a certificate which includes a public key (Col. 22, lines 25 – 62 & Col. 43, lines 18 – 31, the examiner notes that the Clearinghouse and the content providers are connected to the internet and are able to communicate with the end user system, by authorizing a license for the end user to use to view the requested digital content);

- a client apparatus connected to said network, and capable of exchanging data with said server apparatus and receiving

said certificate from said server apparatus (Col. 22, lines 25 – 62 & Col. 43, lines 18 – 31, the examiner notes that the Clearinghouse and the content providers are connected to the internet and are able to communicate with the end user system, by authorizing a license for the end user to use to view the requested digital content);

a key management apparatus connected to said network, said key management apparatus including:

- a first reception unit configured to receive a request for decrypting key information from said server apparatus, said key information including a first key or data which becomes a basis for generating the first key, and said key information being encrypted with the public key by said client apparatus (please see the references abstract, the examiner notes that the client apparatus or user's system has public/private key pair (Col. 82, lines 40 – 52) that allows the user to encrypt

the communications with the clearinghouse which also has private/public key pair, furthermore, clearing house "re-encrypts" the decrypted encrypted information and corresponding decryption key with a second public key, and then it is sent to the user's system, the "second key" is the actual decryption key of the encryption key);

- a first storing unit configured to store a private key which is necessary for decrypting the key information (please see the reference abstract, the examiner notes that the clearinghouse has a first private key that is used to decrypt the encrypted data and the decrypting encryption data key);

- a decryption unit configured to decrypt the key information with the private key and obtain the first key or the data which becomes a basis for generating the first key, after receiving

the request (please see the reference abstract, the examiner notes that the clearinghouse has a first private key that is used to decrypt the encrypted data and the decrypting encryption data key);

- and a first transmission unit configured to transmit to said server apparatus the first key or the data which becomes a basis for generating the first key (please see the reference abstract, the examiner notes that the clearinghouse has a first private key that is used to decrypt the encrypted data and the decrypting encryption data key).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

D.S.H.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER